



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/460,897      | 12/14/1999  | YUNG-KAO HSU         | CASE-1              | 3088             |

7590 10/19/2004

Joseph B Ryan  
RYAN MASON & LEWIS LLP  
90 Forest Avenue  
Locust Valley, NY 11560

| EXAMINER           |              |
|--------------------|--------------|
| TRUONG, THANHNGA B |              |
| ART UNIT           | PAPER NUMBER |
| 2135               |              |

DATE MAILED: 10/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/460,897

Applicant(s)

HSU, YUNG-KAO

Examiner

Thanhnga Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 14 July 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-59 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) 1-21 and 41-59 is/are rejected.
- 7) ☐ Claim(s) 22-40 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-12, 15-17, 41-51, and 54-56 are rejected under 35 U.S.C. 102(e) as being anticipated by Hassell et al (US 6,269, 149 B1).

a. *Referring to claim 1:*

i. Hassell teaches:

(1) said caller sending a communication request message including a communication request for establishing a secure multimedia communication including security information identifying said caller, via said first endpoint to a first one of said Zone Keepers associated with a security zone including said first endpoint [**i.e., this aspect of the invention includes the steps of receiving a signal from a calling party that is requesting the establishment of a communication link (column 3, lines 9-11);**

(2) said first Zone Keeper authenticating the identity of said caller, and if said caller identity is authenticated, authorizing said caller's communication request [**i.e., examining call setup information within the received signal for the second calling party to identify the telephone number of the second calling party. The method further includes the steps of accessing a memory storage area using the telephone number of the second calling party to retrieve information relating to the calling party, and evaluating security data of the retrieved information. If the security data permits the establishment of a**

**connection, then the method establishes a communication link with the calling party (column 3, lines 11-20)];**

**(3) said first Zone keeper determining whether said requested secure communication is an intra-zone or an inter-zone communication [i.e., the step of allocating resources, that is for “determining whether said requested secure communication is an intra-zone or an inter-zone communication”, includes the step of assessing the priority of the second calling party with respect to the first calling party (column 3, lines 36-38)];**

**(4) if said requested communication is an intra-zone communication both said first and second endpoints are in the same security zone, said first Zone Keeper in conjunction with said first and second endpoints in said first security zone establishing said secure communication between said caller and said callee [i.e., referring to Figure 1, in one application of the present invention, the endpoint 14 may be a node in, for example, a corporate environment. In this regard, it may communicate with a local area network 24, that is “an intra-zone communication”, and/or a private branch exchange (PBX) 26 (column 4, lines 48-52)];**

**(5) if said requested communication is an inter-zone communication said first and second endpoints are in first and second security zones, respectively, said first Zone Keeper sending said request message to Said second Zone Keeper associated with said second security zone [i.e., a method for establishing a secured telecommunications link between a calling party and a called party is provided. In accordance with this aspect of the invention, the method includes the steps of receiving a calling from a remote user, identifying the caller identification number, and using caller identification number to access a lookup table (column 2, lines 60-65). In addition, referring to Figure 1, a telecommunications network system, generally designated by reference numeral 10, which connects a first or calling endpoint 12 and a second or called endpoint 14, in communication across a network 16 (column 4, lines 29-33)]; and**

**(6) establishing said secure inter-zone communication utilizing said first Zone Keeper, said first endpoint in said first security zone, said second**

Art Unit: 2135

Zone Keeper and said second endpoint in said second security zone [i.e., the method further confirms from information provided in the lookup table, whether that user is entitled to access the system. If so, then the method directs the system to establish the connection with the remote user. In a preferred embodiment, the system may provide an added level of security by requiring the remote user to enter a password, as well (column 3, lines 1-8). In addition, referring to Figure 1, the entities at endpoints 12 and 14 could be corporate affiliates that communicate regularly across the network 16. In this way, corporate employees that are attached to the network 25 at endpoint 12 may communicate with corporate employees that are attached to the network 24 at endpoint 14 (column 5, lines 21-26)].

b. Referring to claim 2:

i. Hassell further teaches:

(1) providing a capability by each of said Zone Keepers for users of an endpoint in a security zone associated with a particular Zone Keeper to register authentication keys and/or methods and said particular Zone Keeper authenticating said users only through said registered keys and/or methods to honor requests for secure communication [i.e., the primary communications link may be a T1 link, an ISDN link, DDS, DSL, or a POTS link. The link may be a point-to-point link, a permanent virtual circuit, a packet-switched frame relay circuit, or other similar link. Preferably, the system utilizes a lookup table or other database to store party profile information, which may include security information or call priority data. The caller identification number, that is "registered keys", of the calling party is used to access/index such a table or database (column 2, lines 50-58)].

c. Referring to claims 3, 4, 50, and 51:

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

d. Referring to claim 5:

i. Hassell further teaches:

(1) said first Zone Keeper sending an authorization message including an authorization of said caller communication request to said caller, via said first endpoint, said authorization including security information identifying said first Zone Keeper and security information identifying said callee **[i.e., the method further includes the steps of accessing a memory storage area using the telephone number of the second calling party to retrieve information relating to the calling party, and evaluating security data of the retrieved information (column 3, lines 14-18), whereby “first Zone Keeper sending an authorization message including an authorization of said caller communication request to said caller” is inherently provide];**

(2) said caller authenticating the authorization sent by said first Zone Keeper **[i.e., if the security data permits the establishment of a connection, then the method establishes a communication link with the calling party (column 3, lines 18-20), whereby “caller authenticating the authorization sent by said first Zone Keeper” is inherently provided];**

(3) said caller sending, via said first endpoint, a connection request message including a communication proposal for establishing a multimedia communication connection with said callee, via said second endpoint **[i.e., a calling party that is requesting the establishment of a communication link (column 3, lines 10-11), wherein “a communication proposal for establishing a multimedia communication connection with said callee” is considered to include in the request that was sent from the calling party];**

(4) said callee authenticating said authorization and said communication proposal **[i.e., if the security data permits the establishment of a connection (which means “callee authenticating said authorization and said communication proposal”), then the method establishes a communication link with the calling party (column 3, lines 18-20);**

(5) said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that said callee accepts the communication proposal, said message including security information identifying

said callee [i.e., if the security data permits the establishment of a connection (which means "callee accepts the communication proposal"), then the method establishes a communication link with the calling party (column 3, lines 18-20)];

(6) said caller authenticating the identity of said callee [i.e., examining call setup information within the received signal for the second calling party to identify the telephone number of the second calling party (column 3, lines 11-14)]; and

(7) if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints in said first security zone, wherein a secure multimedia communication is established [i.e., preferably, this aspect of the invention includes the steps of receiving a signal from a calling party that is requesting the establishment of a communication link, and examining call setup information within the received signal for the second calling party to identify the telephone number of the second calling party. The method further includes the steps of accessing a memory storage area using the telephone number of the second calling party to retrieve information relating to the calling party, and evaluating security data of the retrieved information. If the security data permits the establishment of a connection, then the method establishes a communication link with the calling party (column 3, lines 9-20)].

e. Referring to claim 6:

i. Hassell further teaches:

(1) if said first Zone Keeper rejects said communication request from said caller, said first Zone Keeper sending an authorization rejected message indicating that said communication request was rejected to said caller, via said first endpoint [i.e., referring to Figure 5, upon receipt of an incoming call (step 102), the system obtains the caller identification information and, through its internal lookup table or database, looks to see if the caller is listed as a valid caller (step 104). The system may also employ password protection. The system then determines whether this caller is one that has a valid access to the system and/or

Art Unit: 2135

checks for a received password to determine whether system access should be granted (step 106). If the caller and/or password is invalid, then the system (at step 108) rejects the call (column 8, lines 25-35)].

f. Referring to claim 7:

i. Hassell further teaches:

(1) wherein said connection request message includes said communication authorization and security information for authenticating the identity of said callee [i.e., referring to Figure 5, the system then determines whether this caller is one that has a valid access to the system, that is "communication authorization", and/or checks for a received password, that is "security information", to determine whether system access should be granted (step 106). If the caller and/or password is invalid, then the system (at step 108) rejects the call. Otherwise, if the caller is a valid caller, it proceeds to step 110 where it determines if the bandwidth on the incoming/outgoing telecommunication link will support the additional caller (e.g., whether a channel is available). If so, then the system proceeds to step 112 where it establishes a connection with the incoming call and returns to step 100 (column 8, lines 30-40)].

g. Referring to claim 8:

i. Hassell further teaches:

(1) wherein said connection message further includes a proposal indicating how the caller-callee communication should be set-up [i.e., referring to Figure 3, a flowchart is provided that depicts the top-level operation of the prioritization aspect of the present invention. Specifically, upon receiving an incoming call, the system validates the call by way of identifying the caller ID (at step 60). This validation step, having been briefly described above, will be described in more detail in connection with FIG. 4. Upon validating the caller ID, the system then determines from an internal database (at step 62) whether it has a prioritization profile for this particular caller ID. In keeping with the description of FIG. 3, if the system detects a valid profile for the caller ID of the incoming call, then it retrieves a profile for that call (step 66). It then checks to determine, based



upon the bandwidth of the incoming link, whether a channel is available to accept the call (step 68) (column 7, lines 11-20 and lines 30-34)].

h. Referring to claim 9:

i. Hassell further teaches:

(1) said first Zone Keeper employing a prescribed security arrangement for authenticating the identity of said caller [i.e., referring to Figure 5, upon receipt of an incoming call (step 102), the system obtains the caller identification information and, through its internal lookup table or database, looks to see if the caller is listed as a valid caller (step 104). The system may also employ password protection. The system then determines whether this caller is one that has a valid access to the system and/or checks for a received password to determine whether system access should be granted (step 106) (column 8, lines 25-34)].

i. Referring to claim 10:

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

j. Referring to claim 11:

i. This claim has limitations that is similar to those of claims 7 and 8, thus it is rejected with the same rationale applied against claims 7 and 8 above.

k. Referring to claim 12:

i. Hassell further teaches:

(1) wherein said connection request message further includes security information for authenticating the identity of said callee [i.e., of course, as an added means of protection, a system endpoint could require not only that a call be placed from particular caller ID locations, but also that the calling party enter an appropriate password, as a secondary level of security and protection (column 5, lines 63-67)].

l. Referring to claim 15:

i. Hassell further teaches:

(1) said first Zone Keeper forwarding said communication request message to a second Zone Keeper associated with said second security zone [i.e., referring to Figure 1, "first Zone Keeper forwarding said communication request message to a second Zone Keeper associated with said second security zone" is considered to include in a telecommunications network system 10, whereby a first endpoint 12, that is "first Zone Keeper", and a second endpoint 14, that is "second Zone Keeper"];

(2) said second Zone Keeper authenticating that the communication request message is from said first Zone Keeper [i.e., caller identification information is utilized for purposes of enhancing system security. In this regard, a given endpoint, for example, 14 would be preconfigured, that is for "authenticating that the communication request message is from said first Zone Keeper", to accept calls only from certain predefined users, and more specifically, from predefined endpoints for backup purpose (column 5, lines 57-60)];

(3) said second Zone Keeper sending an authorization message including an authorization of said caller communication request to said first Zone Keeper, said authorization message including security information identifying said second Zone Keeper and security information identifying said callee [i.e., referring to Figure 1, "second Zone Keeper sending an authorization message including an authorization of said caller communication request to said first Zone Keeper" is considered to include in a telecommunications network system 10, whereby, as an added means of protection, a system endpoint could require not only that a call be placed from particular caller ID locations, but also that the calling party enter an appropriate password, as a secondary level of security and protection (column 5, lines 63-67)];

(4) said first Zone Keeper authenticating the authorization in said authorization message sent by said second Zone Keeper [i.e., referring to Figure 1, "first Zone Keeper authenticating the authorization in said authorization message" is considered to include in a telecommunications network system 10];

(5) if said authorization in said authorization message is authenticated, said first Zone keeper sending said authorization message to said caller via said first endpoint **[i.e., referring to Figure 1, “first Zone keeper sending said authorization message to said caller via said first endpoint” is considered to include in a telecommunications network system 10];**

(6) said caller sending, via said first endpoint, a connection request message including a communication proposal for establishing a secure multimedia communication connection with said callee, via said second endpoint **[i.e., a calling party that is requesting the establishment of a communication link (column 3, lines 10-11), wherein “a communication proposal for establishing a multimedia communication connection with said callee” is considered to include in the request that was sent from the calling party];**

(7) said callee authenticating said authorization and said communication proposal **[i.e., if the security data permits the establishment of a connection (which means “callee authenticating said authorization and said communication proposal”), then the method establishes a communication link with the calling party (column 3, lines 18-20);**

(8) said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that callee accepts the communication proposal, said message including security information identifying said callee **[i.e., if the security data permits the establishment of a connection (which means “callee accepts the communication proposal”), then the method establishes a communication link with the calling party (column 3, lines 18-20)];**

(9) said caller authenticating the identity of said callee **[i.e., examining call setup information within the received signal for the second calling party to identify the telephone number of the second calling party (column 3, lines 11-14)];** and

(10) if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints, wherein a secure multimedia communication is established **[i.e., preferably,**

Art Unit: 2135

this aspect of the invention includes the steps of receiving a signal from a calling party that is requesting the establishment of a communication link, and examining call setup information within the received signal for the second calling party to identify the telephone number of the second calling party. The method further includes the steps of accessing a memory storage area using the telephone number of the second calling party to retrieve information relating to the calling party, and evaluating security data of the retrieved information. If the security data permits the establishment of a connection, then the method establishes a communication link with the calling party (column 3, lines 9-20)].

m. Referring to claims 16, 42, and 55:

i. These claims have limitations that is similar to those of claim 6, thus they are rejected with the same rationale applied against claim 6 above.

n. Referring to claim 17:

i. Hassell further teaches:

(1) said first Zone Keeper determining whether said caller and said callee are security compatible for the requested secure multimedia communication [i.e., referring to Figure 1, "said caller and said callee are security compatible for the requested secure multimedia communication" is considered to include in a telecommunications network system 10].

o. Referring to claim 41:

i. This claim has limitations that is similar to those of claims 1 and 5, thus it is rejected with the same rationale applied against claims 1 and 5 above.

p. Referring to claim 43:

i. These claims have limitations that is similar to those of claim 7, thus they are rejected with the same rationale applied against claim 7 above.

q. Referring to claim 44:

i. These claims have limitations that is similar to those of claim 8, thus they are rejected with the same rationale applied against claim 8 above.

r. Referring to claim 45:

Art Unit: 2135

i. These claims have limitations that is similar to those of claim 9, thus they are rejected with the same rationale applied against claim 9 above.

s. Referring to claim 46:

i. These claims have limitations that is similar to those of claim 10, thus they are rejected with the same rationale applied against claim 10 above.

t. Referring to claim 47:

i. These claims have limitations that is similar to those of claim 11, thus they are rejected with the same rationale applied against claim 11 above.

u. Referring to claim 48:

i. These claims have limitations that is similar to those of claim 12, thus they are rejected with the same rationale applied against claim 12 above.

v. Referring to claim 49:

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

w. Referring to claim 54:

i. This claim has limitations that is similar to those of claims 1, 15, and 17, thus it is rejected with the same rationale applied against claims 1, 15, and 17 above.

x. Referring to claim 56:

i. These claims have limitations that is similar to those of claim 17, thus they are rejected with the same rationale applied against claim 17 above.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2135

4. Claims 13-14, 18-21, 52-53, and 57-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hassell et al, and further in view of Patel (US 6, 327, 660).

a. Referring to claims 13, 14, 18, 19, 20, and 21:

i. Hassell teaches the claimed subject matter except for:

(1) said first Zone Keeper providing authentication of its identity by using public-key cryptography and a digital signature and wherein said users authenticate the first Zone Keeper identity by employing said first Zone Keeper's public key.

(2) obtaining said digital signature by said first Zone Keeper signing said request response message with a private-key.

(3) wherein each of said Zone Keepers has its own private key, and further including said first Zone Keeper signing said 3' communication request message and said second Zone Keeper authenticating that said communication request message was sent by said first Zone Keeper through said first Zone Keeper's private key.

(4) wherein each of said Zone Keepers has its own digital signature, and further including security information indicating the identity of said callee and said second Zone Keeper including its digital signature in said authorization message sent to said first Zone Keeper, and said first Zone Keeper authenticating the authorization sent by said second Zone Keeper through the digital signature of said second Zone Keeper.

(5) wherein each of said Zone keepers has its own public key, said caller authenticates said authorization by verifying said digital signature of said first Zone Keeper and said callee authenticates said authorization and communication proposal by verifying the digital signature of said second Zone Keeper through its public key.

(6) wherein each of said users has its own password which is registered by the user of an endpoint with the endpoint's associated Zone Keeper, and each of said Zone Keepers has its own private key and its own public key

and further including said communication request message including a first prescribed security token, said first Zone Keeper authenticating said first prescribed security token, and if said first prescribed security token is authenticated, determining that said communication should be allowed.

ii. Patel teaches:

(1) Referring to Figure 7, security association 700 can be established through several schemes. For example, the first electronic system may be pre-configured with an appropriate security association. In this situation, first electronic system is loaded with an address of the second electronic system, SPI, and keys (e.g., public key, private key, secret key, etc.) for encryption and decryption of information, inclusive of digital signatures. In some embodiments, however, multiple security associations are stored in the first electronic system and are used in some predetermined order so that different keys are used at different times (column 6, lines 16-25).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such security association 700 (in Hassell) since the digital signature is used to protect the integrity of data by avoiding its illicit modification and is used to identify the source of data. In the alternative, a digital signature could be obtained by computing a hash of the data concatenated with a secret key. A "digital certificate" includes a source identifier (e.g., public key, serial number, etc.) encrypted with a private key of a certification authority. Examples of a "certification authority" include a manufacturer, a trade association, a governmental entity, a bank or any other entity in a position of trust by the consumer (column 3, lines 10-19 of Patel).

iv. The ordinary skilled person would have been motivated to:

(1) add such security association 700 (in Hassell) because a communication channel is considered to be "secure" when (i) the modification of data transmitted through the communication channel can be detected, and (ii) the source of the transmitted data can be authenticated, and/or the confidentiality of the transmitted data is protected. Cryptographic techniques such as

Art Unit: 2135

digital certificates, digital signatures, and the encryption/decryption of data are used to secure a communication channel (column 1, lines 24-31 of Patel).

b. Referring to claims 52, 53, 57, 58, 59:

i. These claims have limitations that is similar to those of claims 13, 14, 18, 19, and 20, thus they are rejected with the same rationale applied against claims 13, 14, 18, 19, and 20 above.

***Allowable Subject Matter***

5. Claims 22-40 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Response to Argument***

6. Applicant's arguments filed July 14, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

"The Hassell reference relied upon by the Examiner fails to meet the above-noted limitations of independent claim 1. For example, there is no mention whatsoever in Hassell regarding the claimed security zones, each having an associated Zone Keeper, or the claimed determination as to whether a given requested secure communication constitutes an intra-zone or inter-zone communication. Thus, Hassell fails to teach or suggest a dual-tier security architecture of the type claimed."

Examiner maintains that:

Hassell teaches the claimed subject matter. In fact, turning now to Figure 3, a flowchart is provided that depicts the top-level operation of the prioritization aspect of the present invention. Specifically, upon receiving an incoming call, the system (that is "a zone keeper") validates the call by way of identifying the caller ID (at step 60). This validation step, having been briefly described above, will be described in more detail in connection with Figure 4. Upon validating the caller ID, the system then determines from an internal database (at step 62) whether it has a prioritization profile for this particular caller ID. If not, it rejects the incoming call (step 64) (column 7, lines 11-20). Furthermore, Hassell states that there are, however, various shortcomings in the



Art Unit: 2135

present state of the art, including the handling of fault detection, security, and call prioritization. Mechanisms are well known for identifying and notifying a user of a line breakage or other fault condition existing in the link between endpoints. However, endpoint equipment often responds by rerouting all data on a particular line, as opposed to on the affected data. For example, suppose one endpoint of a telecommunications network interfaces to a local area network (e.g. a corporate network) and the telecommunications link communicating with the endpoint is a high capacity T1 line, whereby local area network is "an intra-zone". In addition, another shortcoming noted in present state of the art systems relates to security. In keeping with the previous example of telecommunications network endpoint being connected to a local area network, there is a tremendous need for providing a secured entry from any caller outside the local area network (that is "an inter-zone") to access the network by way of, for example, a dial-up connection. Frequently security issues, such as this one, are handled by password protection. In such systems, dial-up users are required to provide a password for access to the network (column 1, lines 35-67). Beside, the terminology "a dual-tier security" that applicant mentioned in the remark does not even address in the claim language as set forth in independent claims 1, 41, and 54.

Applicant further argues that:

"The Patel reference cited by the Examiner fails to overcome the fundamental deficiencies of Hassell as applied to the independent claims. Thus, the proposed combination fails to teach or suggest all the claim limitations" as is required for establishment of a proper prima facie case."

Examiner disagrees with the remark and still maintains that:

Sufficient reason of combining has been given in the rejection: Cryptographic techniques such as digital certificates, digital signatures, and the encryption/decryption of data are used to secure a communication channel (column 1, lines 24-31 of Patel).

### **Conclusion**

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See

Art Unit: 2135

MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

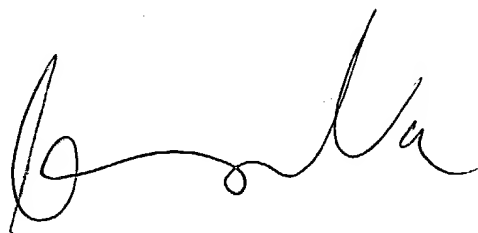
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TC 2100 will be moved to Carlyle in October 2004, the new telephone number for TC 2100 receptionist is 571-272-2100. In October 2004, any inquiry concerning this communication should be directed to Thanhnga (Tanya) Truong whose new telephone number is 571-272-3858, and the examiner's supervisor, Kim Vu can be reached at 571-272-3859.

TBT

October 13, 2004



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100